

Project : Firewall Log Analyzer and Monitoring Application

ABSTRACT

The continuous growth of networked systems has resulted in the generation of large-scale firewall logs that are difficult to analyze manually and in real time. Traditional log monitoring methods rely heavily on command-line inspection, which limits the timely detection of security threats and increases operational complexity. This study focuses on addressing the need for automated firewall log analysis to improve network security visibility and response efficiency. The objective of the proposed system is to identify malicious activities within firewall logs and provide timely alerts without requiring manual intervention. The system processes firewall logs collected from Linux-based environments and applies rule-based and machine-learning-assisted analyses to recognize suspicious patterns, such as repeated authentication failures, port scanning behavior, and unauthorized service access. An optimized log storage strategy using MongoDB enables continuous data ingestion via automated log retention. A web-based interface supports real-time monitoring, filtering, and the generation of reports. Experimental observations show that the system enhances the threat detection speed and reduces the response latency compared with conventional manual-logging analysis. The proposed approach contributes to scalable and efficient security monitoring, demonstrating the practical benefits of automated firewall log analysis in modern network environments.